Security Architecture and Design Documentation Guidance

DESCRIPTIVE TOP LEVEL SPECIFICATION

Version 1.0

Prepared by HR CDS TT

21 June 2011

REVISION HISTORY

Name	Date	Reason For Changes	Version
HRCDSTT	21 June 2011	Document creation	1.0

ACRONYMS AND DEFINITIONS

Acronym	Definition
CDS	Cross Domain Solution
DRD	Data Representation Documentation
DTLS	Descriptive Top-Level Specification
FTLS	Formatl Top-Level Specification
HLD	High Level Design
LLD	Low Level Design

INTRODUCTION

A Descriptive Top-Level Specification (DTLS) is a description of system security function behavior at it is visible at external interface. It is at the most abstract level[1]. It describes the external interfaces in detail while omiting any implementation details. The DTLS is also known as an Informal Top-Level Specification[2]. The DTLS is employed in the development of high robustness and medium-robustness systems. The DTLS is derived from information contained in the High Level Design (HLD) (see Figures 1 and 2 (next page)). The DTLS provides data for the Low Level Design, the Covert Channel Analysis. The DTLS just be consistent with the HLD and the FTLS (for High Robustness).

GOAL

The goal of the FTLS is to:

- provide information to the implementers for the design the low level design and the implementation representation
- provide a translation of the FTLS that can be used by the implementers as a description of the interfaces and behaviors of the system
- provides tracability from the implementation to both design and the specifications

DISCUSSION

The DTLS is a key component of the development process and the corresponding independent confirmation process. The DTLS is an informal top-level specification of the interfaces of the security functions. The DTLS must be clear, accurate, complete, and consistent with the other documentation.

The DTLS must completely and accurately define all effects and exceptions visible at the external security interface resulting from any sequence of control/data entries to the interface with any combination of parameters. The DTLS can define effects without describing or listing all of them. The DTLS should describe initial and default states of each interface. The description for each interface the impact inputs have on the state of the interface. An interface can affect other entry interfaces when the inputs are made in certain sequences and the resulting behaviors should be described. In cases where input events create delayed security relevant effects, they must be described.

---

[1] "Most abstract level" means no internal components or algorithms are used in the description, otherwise the definition is self-contradictory.

[2] Informal Top-level Specification for Trusted Application Systems, J. P. McDermott, J. N. Froscher, C. N. Payne, and H.O. Lubbes, Proceedings of the Sixth Annual Computer Security Applications Conference, 3-7 December 1990

REQUIREMENTS

DTLS-1 The developer shall provide the descriptive top-level specification (DTLS) for the system.

DTLS-2 The DTLS shall be written in an informal language natural language (as specified in the DRD), an informal program design notation, or a combination thereof.

DTLS-3 The DTLS shall describe all of the external interfaces of the security functions including inputs, outputs, exceptions, error messages, and effects.

DTLS-4 The DTLS shall be internally consistent.

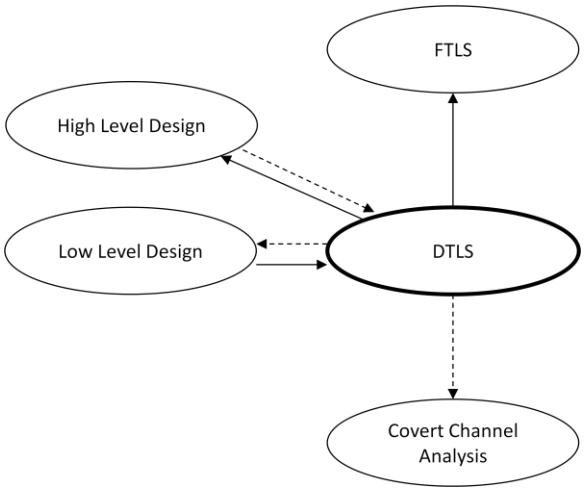

Figure 1 – DLTS Relationships for High Robustness

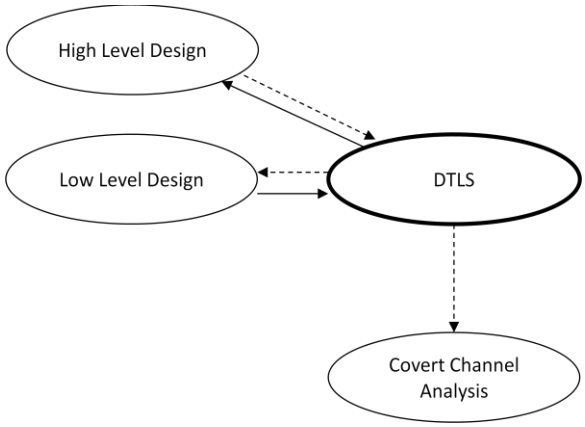

Figure 2 –DTLS Relationships for Medium-High Robustness